SECOM-357D-82
file 3.1

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
Unauthorized Disclosures of Classified Information

25X1

FROM:
Chairman, SECOM

EXTENSION

NO.
SECOM-D-357

DATE
1 November 1982

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. D/OCC/ICS	11/3/82			
2.				
3. D/ICS				
4. ER	11/29/82	11/29/82		
5. DDCI				
6.				
7. DCI				7. For approval
8.				
9. C/SECOM 7B31				
10.				
11.				
12.				
13.				
14.				
15.				

DCI EXEC REG

FORM 1-79 610 USE PREVIOUS EDITIONS

INTELLIGENCE COMMUNITY STAFF

Ch/Secom

25X1 [redacted]

Returned at your request.

It can be recycled at anytime. Please note

25X1 [redacted] remarks to

25X1 [redacted] I think they are quite supportive.

Let me know (and

25X1 [redacted] too) when and if you decide to move it along.

25X1 [redacted]

ACTION

Director
Intelligence Community Staff
Washington, D.C. 20505

20 JAN 1983

NOTE FOR: DDCI

John -

25X1
25X1

I have just had a good discussion with [redacted] on the leak problem and their proposals to address it. I think that the subject deserves your attention and recommend a session like the one I have just had with Bob to explore the problem and the means by which we can do something about it. Bob's paper provides a good basis for such a discussion.

I particularly favor the leak damage study Bob is proposing, but I think it would be more effective if it were to be done as a government, rather than a contractor, effort. Also, I think the leak data base idea has some merit and might possibly be done with in-house ICS resources. I am not as comfortable with the proposal to add positions in the FBI to investigate leaks. We need more study and more high-level inter-agency coordination on this topic before proceeding, especially considering the difficulty of adding manpower to the FBI.

25X1

I strongly recommend you schedule some time with [redacted] and me to talk about this. I think you will agree that it is a subject worthy of the DCI's attention, but we need to have a fuller set of proposals to consider before approaching him. I'll be glad to join you w/Bob if you desire

25X1

[redacted]

Unauthorized Disclosures of Classified Information

The most persistent security problem in the US Government is that of unauthorized disclosures of classified information (leaks). The Attorney General has sent to the President a report of an interdepartmental group, recommending a number of actions to alleviate this problem.

This report, which has the complete endorsement and support of the DCI Security Committee and the Unauthorized Disclosures Investigations Subcommittee, recommends:

- Legislation to criminalize the unauthorized disclosure of properly classified information by a government employee.

- Greater use of properly drafted secrecy agreements to provide civil sanctions for leaks.

- Better security education for senior officials (SECOM recently produced a videotape introduction to security for senior officers).

- Better controls on copying and circulation of classified documents. (Unfortunately, sensitive intelligence has an increasing audience, all of whom have a legitimate claim to the information.)

- Updating of Executive Order 10450 and the federal personnel security program. (EO 10450 was issued in 1953.)

- Adoption of appropriate policies governing contacts between media representatives and government officials.

- Internal agency procedures to ensure effective investigations of leaks and the imposition of appropriate sanctions.

- Investigation of leaks by the FBI in cases where a successful investigation will probably result in Administrative sanctions rather than prosecution. (This is a key proposal. Investigation of leaks by the FBI, instead of multiple agency investigations of the same leak, is certain to be more effective. SECOM has voted to offer the services of the Unauthorized Disclosures Investigations Subcommittee to assist the Department of Justice in screening leaks for potential investigation by the FBI.)

SECRET

- Modify existing restrictive government regulations to permit the use of polygraph examinations for government employees in leak investigations.

The Security Committee has consistently supported efforts to have the FBI conduct leak investigations. Few leaks occur entirely within a single agency - usually one agency collects information, another analyzes and reports it and still others consume the reports. The fragmented approach of having each agency conduct its own investigation is seriously flawed. Although the FBI doesn't have the resources to investigate every leak, the successful investigation of selected leaks and subsequent penalities to the leakers should have a salutary effect upon other potential leakers.

The Security Committee has sought resources to assemble an interagency leak data base which would assist not only in evaluating individual leaks but would for the first time provide a means of quantifying the leak problem. There is no central record of how many leaks have occurred and there is no way to coordinate recurring leaks from the same documents are sources. If such a data base could successfully be assembled, it would provide for a mosaic approach to investigation and identification of the sources of leaks.

The SECOM has also sought resources to conduct a study of the origin, nature and consequences of leaks. Here again, there is no coordinated body of information upon which to base evaluations of leaks, including the number of times specific information has been published, the probable source of such information and the loss incurred as a result of leaks.

The above recommendations would, if implemented, provide the ability to size the problem, create a diagnostic tool to assess correlation between leaks and publications, and provide continuity and order to the leak investigation effort. They would also assist in identifying security vulnerabilities and provide focus to the effort, which is now completely decentralized.

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-357
1 November 1982

MEMORANDUM FOR: Director of Central Intelligence

VIA: Deputy Director of Central Intelligence
Director, Intelligence Community Staff

STAT FROM: [redacted]
Chairman

SUBJECT: Unauthorized Disclosures of Classified Information

1. Action Requested: DCI support for three recommendations intended to provide at least modest action toward determining the sources of unauthorized disclosures of classified information. A fourth recommendation encourages continued DCI support of the Willard Report.

2. Background: The problem of leaks--disclosures of classified intelligence to the news media or other unauthorized persons--is the oldest, most frustrating, and most unmanageable problem facing the DCI Security Committee. The SECOM first came together in 1959 to seek a way to deal with leaks. On untold occasions since then, senior officials of the government have decried the apparent impossibility of keeping a secret in Washington.

3. The number of studies of how to stop leaks, or to identify and penalize leakers, is exceeded only by the number of leaks that have occurred. The situation grows worse because of the ambivalence about leaks in the highest levels of government. On one hand, leaks are despicable because they foreclose the options of the policy makers and/or jeopardize the national security. On the other hand, a well-placed leak can be used to enhance greatly the image of the leaker, his programs and policies or to seriously discredit his adversaries or their programs and policies. The leak is a two-edged sword, not easily surrendered by those who feel the need to influence public opinion.

4. As Winston Churchill and others have observed, "The Ship of State is the only vessel that leaks at the top." It is generally believed that most disclosures of classified data are made by persons who (a) are knowledgeable, (b) have trusted contacts in the media, and (c) have motivation, selfish or political. Few, if any, minor bureaucrats possess all of these characteristics. Even if a "leaker" is found, he may have sufficient support from influential friends to avoid being penalized.

5. The procedure for investigating leaks of sensitive intelligence information has been unchanged for at least two decades. First, a determination is made that sensitive information has been disclosed. The document from which the compromised information came is then identified and the authorized dissemination of the document is determined. In the typical case, the dissemination is found to be well into the hundreds, with recipients in several departments and agencies, both within and outside the Intelligence Community. With everyone who saw the hundreds of documents a potential suspect, and with the inability of agencies to investigate outside their own organizations, the situation is normally declared hopeless and the investigation is dropped. In some cases, a few people will be asked whether they were the source of the leak. They promptly deny responsibility, and the matter is closed. If anything has been proven in a quarter of a century of trying, it is that this procedure does not work.

6. It has been suggested that the successful investigation of only a few cases, resulting in well-publicized and appropriately severe penalties, could drastically change the attitude of the federal bureaucracy toward leaks. Many have thought that having the Federal Bureau of Investigation investigate leaks would be an ideal solution to the problem. This is hampered by the Justice Department's requirement that the agency requesting the investigation answer a series of questions, one of which is whether the leaked information can be declassified to permit prosecution. This places the complaining organization in the position of either declassifying the information and insuring its confirmation and further dissemination, or declining to declassify, insuring that the FBI will not undertake the investigation. Even under ideal conditions, the FBI would not have the resources to investigate each leak that occurs. Therefore, a process for selecting the leaks worthy of investigation is needed.

7. A leak rarely is a one-agency phenomenon. Typically, information is gathered by one agency or more, analyzed and turned into finished intelligence by one or more others, and then disseminated to the entire Intelligence Community (and sometimes to agencies outside the IC). Any effective leak investigation must cross agency lines and do so quickly. Delays or failures resulting from lack of resources, lack of interest, or simple inefficiency in any agency or department can be fatal to the investigative effort. Yet it is the nature of bureaucracy that no department or agency head will willingly allow investigators from another agency to conduct inquiries on his turf. The vigor with which internal investigations are pursued may be tempered by fear of the embarrassment that would result from finding a "leaker" within one's own agency or department, or by the attitude that the problem is really someone else's. Any solution to the problem requires an investigative organization whose jurisdiction throughout the government is recognized and accepted. Only the FBI meets this criterion.

8. The tools available for investigating leaks are inadequate. Not only are there far too few investigators, whose charters are hopelessly narrow, but

there is no useful data base to aid probers. Funds have been sought without success to assemble a Community-wide computerized register capable of electronically sorting leaks by topic, publication, organizations having access, identity of reporter, dates of publication, etc. The possibility of constructing a mosaic which could point toward a leaker would be greatly enhanced by such a program. Nor is there any capability in the Community for a long-term analytical study of leaks. Instead, leak investigation is a reflexive activity, stimulated by the publication of sensitive data, and resulting each time in the stylized "kabuki dance" response described earlier in paragraph 5.

9. Perhaps just as debilitating is the inability to use certain investigative techniques without risking the wrath of the fourth estate. Polygraph testing can be done with relative impunity only by CIA and NSA because their employees are routinely tested. Wiretapping, a perfectly respectable investigative technique when done with the necessary legal sanctions, is out of the question politically. Physical surveillance is about as bad. The net effect is a contest in which the advantages are all on the side of the leaker, while the investigators must bear disabling handicaps.

10. The real issue is whether the Government is serious about leaks. Willingness to pay the price for stopping them has not existed heretofore. And a steep price it is, indeed. It would mean government officials would have to give up trying to manipulate the media. (Maybe the price is not so high in this regard, as it seems the media always come out ahead.) It would also mean that government officials would have to endure considerable abuse from the media, which would try to make a First Amendment issue of any serious effort to curtail leaks. The original text of NSDD-19 was directly on target, but the Washington Post reported its issuance before it could be disseminated fully. Its immediate rescission reflected the serious concern of the Administration with the dire consequences of a policy that inevitably would be labeled by the media an attempt to abridge the First Amendment rights of Federal employees. It is clear that there is no way to shut down the torrent of leaks in a manner that will please the media.

11. Among measures which should be considered to try to give the investigators an even break with the leakers is a firm policy prohibiting Executive Branch personnel from giving information to the media without attribution. They should be required to insist upon being identified as the source of the information, and anyone providing information without attribution would be in violation of this policy and subject to penalties. As insurance against appearing to violate this rule, officials should be encouraged to report all contacts with the media to a designated component of their own departments or agencies. For those situations where a leak is believed to be in the national interest, a focal point to register and clear leaks could be established in the Executive Office of the President or the National Security Council. This would separate the so-called "official leaks" from the inadvertent or deliberate disclosures committed by individuals on their own.

12. It is ironic that one of the most vigorous, and possibly most successful, leak investigations in recent memory concerned the revelation of UNCLASSIFIED deliberations of the Defense Resources Board in spring 1982. All those attending the board meeting were polygraphed, and the culprit apparently identified. External factors caused his punishment to be commuted. But the case proved that unauthorized disclosure cases can be solved if resources are brought to bear and sound investigative tools are used.

13. Legislation is needed to criminalize unauthorized disclosures of classified intelligence by Federal employees even when a foreign government is not the recipient, but its enactment is extremely unlikely. No one has been successfully prosecuted under the Espionage Statutes for an unauthorized disclosure, as distinguished from providing information to a foreign power. An Executive Branch policy requiring reporting of all media contacts by persons with access to classified information seems remote, given the fate of the original NSDD-19. The only adjustment in the leak investigation procedure that seems practicable is to provide the FBI with the marching orders and the manpower to investigate the publication of classified information. The goal of the investigation need not be prosecution. It could be the enhancement of the national security by determining how the leak occurred and taking corrective measures. If the investigation results in the identification of the Federal employee responsible for the leak, then the possibility of prosecution or administrative sanctions can be considered. Meanwhile, steps can be taken to shore up any weaknesses in security policy or practice uncovered by the investigation.

14. The SECOM has requested, most recently in the FY 1984 budget submission, funding for a Community-wide leak data base and for a study of the origins, nature and consequences of leaks. The lack of success of this initiative may reflect the true attitude of the Community--that leaks are worth bemoaning but not worth the expenditure of funds. It is essential that we try to quantify and qualify the leak problem. This can be done only by assembling a body of information upon which to base evaluations of leaks, including how many times specific information has been published, the most likely sources, and what has been lost as a result of leaks. It is not my purpose to flog a dead horse, but I strongly feel that further delay of an empirical approach to leak evaluation and investigation dooms us to continue repeating the mistakes of the past.

15. The SECOM, at its recent seminar, voted to try to assemble a task force to review a limited area of intelligence activity to determine the extent of damage resulting from leaks. This effort will be handicapped by the lack of a data base but will rely upon its narrow focus to seek appropriate conclusions. If the effort is successful, it will prove that a data base is vital to a broad review of the nature of the leak phenomenon and to any progress toward a solution. The SECOM also voted unanimously to recommend that the DCI offer to the Attorney General the services of the Unauthorized Disclosures Investigations Subcommittee to assist in evaluating and prioritizing leaks for investigation by the FBI.

16. A word of caution. The FBI is not eagerly seeking this task--it is thankless, places the organization's public relations at risk, and has no guarantee of success. It offers, however, the possibility of breaking the impasse we reached long ago. The Bureau is not likely to accept the job without additional manpower, and even then acceptance will be reluctant. Nor does providing funds for the creation of a leak data base assure us of putting a stop to leaks. But the data base is a tool without which we cannot hope to understand, let alone solve, the leak problem. Unfortunately, some of those who complain loudest about leaks seem least willing to share their resources to combat them. It is time for us to put up or shut up.

17. The Willard Report, prepared by a committee headed by the Department of Justice, contains many useful recommendations to help remedy the unauthorized disclosure problem. The report is a wide-ranging document, however, and is still being mulled over by the NSC Staff. This paper recommends action which can be undertaken in the near future and which can be accomplished without legislation or massive funding.

18. Recommendation: That the DCI:

a. Sponsor, in consultation with the Director, FBI and the Attorney General, an initiative calling on the FBI to investigate selected leaks whether or not prosecution is expected to ensue, and providing additional manpower to offset FBI personnel requirements to conduct leak investigations. Approximately 12 positions should provide a respectable level of effort. The DCI should be prepared to provide advice on the selection of leaks for investigation in order to keep the FBI workload within manageable limits.

b. Reprogram FY 1983 NFIB funds ($250,000 and 3 positions),and plan for similar resources in FY 84 and beyond, to provide the Security Committee the means to establish and maintain a computerized, Community-wide, leak data base for use in analyzing leaks for patterns or trends.

c. Reprogram FY 1983 NFIP funds ($125,000) to provide the Security Committee resources needed to contract an analytical study of the long-term effects and characteristics of leaks.

d. Continue vigorous support of the findings and recommendations of the Willard Report.

STAT

SUBJECT: Unauthorized Disclosures of Classified Information

APPROVED: Recommendation A

Director of Central Intelligence — Date

APPROVED: Recommendation B

Director of Central Intelligence — Date

APPROVED: Recommendation C

Director of Central Intelligence — Date

APPROVED: Recommendation D

Director of Central Intelligence — Date

Distribution:
Orig - Return C/SECOM
1 - DCI
1 - DDCI
1 - ER
1 - D/ICS
1 - D/OCC/ICS
1 - ICS Registry